Assignment 1

The Basics

Networking Fundamentals

1. Consider the following scenario
   Suppose, you are a network consultant advising a medium-sized manufacturing company with departments spread across three floors. The current network setup is becoming inefficient, and the company is looking to revamp its infrastructure. Your task is to recommend a suitable network topology (among star, bus & ring), considering factors like data transfer efficiency, fault tolerance, scalability, and ease of management. Provide a brief analysis of the chosen topology's advantages and disadvantages, along with real-world examples where this topology has been successfully implemented. Consider cost implications and potential challenges in your recommendations.

   Ans: Among the three mentioned topologies, star topology would be the best choice considering data transfer efficiency, fault tolerance, scalability, and ease of management.

   Firstly, each node in a star topology is connected to a central network hub it is ideal in a star topology to provide the best efficiency in data transfer. In the case of fault tolerance, star topology would be ideal to use. For example, if one computer is disconnected from the network, other computers will not be hampered and won't see the network won't see downtime. For medium-sized companies like the above scenario, it is crucial to not have any downtime. Moreover, a star topology network is highly scalable. One needs to only connect new computers to the central network hub or switch to get connected with the rest of the network. Furthermore, a network based on star topology is easier to maintain due to the centralization of the network. We can easily manage everything under the network from the central hub, so management, performance monitoring, and troubleshooting would be easy to execute. Lastly, due to the centralized nature, the use of hub and switches is less compared to bus and ring topologies where these are used mostly. For a medium-sized business, the cost would be to use more buses and switches. So, there is only the need to use more network cables which cost less compared to hubs and switches.

   The advantages and disadvantages of the **star topology** are discussed with real-world examples, in the following table:

Advantages	Disadvantages
1. Easy to install and wire new PCs to the network due to the centralized system.	1. Dependency on centralization gives scope to single-point of failure. If the central hub is offline or hacked, then all the data can get in trouble.
2. Offers high scalability as it is easy to add or remove any PCs. We just have to disconnect from the central system.	2. Even though we can cost, by minimizing the use of hubs and switches, there will be a cost for adding more cables. Also, there could be a limitation for using cable length between the PCs and the central hub.
3. It is to manage all devices and troubleshoot any problem under the network. If there are any errors in hubs and switches we can specifically understand where the problem is in star topology.	3. As the pressure on the central hub is more due to all the network traffic going through, it needs more maintenance than a normal hub, when adding new PCs to it. This can sometimes cause minor downtime or restart of the network.
4. Due to the central hub, it can efficiently manage network traffic flow inside the network.	
5. We do not need a lot of switches or hubs to update the network. Just by adding cables to the new PCs with the central hub, we can connect the PCs. This cuts costs and provides efficiency.	

2. Research and outline three common network security threats and propose preventive measures to mitigate each threat.

   Ans: The three most common network security threats are Phishing, Ransomware, and DDoS attacks.

   Phishing attack: The type of network security threat that deceives people into giving personal information by pretending to be a trustworthy company.

Preventive solutions for these threats are to make people aware of these sorts of messages or emails, use advanced email filtering to detect any phishing emails and use anti-phishing applications and browser extensions.

Ransomware attack: Ransomware attacks when someone installs unknown software or downloads any file that might contain malware that would when executed encrypt files and demand payment for decryption.

Possible measures which we could take to prevent ourselves from getting these sorts of attacks are mainly to be careful before downloading any software and verifying the authenticity of it, using antivirus software which has real-time protection, and backing up our important files from time to time in somewhere safe.

DDoS attack: Distributed Denial of Service or DDoS in short attacks overwhelm the networks with traffic, disrupting the service.

Preventive measures that we can take to stop these sorts of attacks are using a captcha solution on our website, limiting the rate of requests a server accepts from an individual IP address, and blocking communication of the server from outdated ports, or applications.

Operating System Knowledge (Linux)

1. Provide a step-by-step guide on how to change file permissions on Linux.

Ans: A step-by-step guide on how to change file permissions on Linus PC is as follows:

a. First, we have to open the Terminal program.

b. Then we have to go to the location where the current file is located using the **cd** command.

c. After going to the destination folder we need to type **chmod** command followed by the desired permissions ending with the filename including the extension. For example, if we were to give a user read, write, and execute access then the command will be **chmod u+rwx filename.extension**

d. If it is for any groups or others then we simply have to use **chmod g+rwx filename.extension** or **chmod o+rwx filename.extension**

e. We have to be careful with the extension part as there could be two files with the same name but different extensions.

2. Imagine a Linux server experiencing high CPU usage. Research and outline the commands and techniques used for monitoring and managing processes on Linux. Provide a detailed explanation of how to identify and terminate processes consuming excessive system resources.

   Ans: The commands that we can use to monitor and manage processes on Linux are as follows:

   top command: It provides a real-time view of the running process, including CPU and RAM usage.

   htop command: it is similar to the top command but updated to be more user-friendly with the support of process tree view and process management where we can control what to do with a process.

   vmstat command: It displays information about process, memory, block I/O, paging and CPU activity which is needed for an depth understanding for processes management and monitoring.

   Now, to identify the process with high CPU usage we can use any of the commands above and identify the Process ID or PID of the process. Once we have identified the processes with high CPU percentage and get its PID. We can run the command **kill PID-value** and the processes will be terminated. Sometimes, there can be the same processes that have more than one instance. So, even if we terminate one process the high CPU usage might not stop due to other instances running. So, in that case, we have to run **killall process-name** command to ensure all the instances that match the process name will be terminated.

3. Provide a step-by-step guide on how to install, update, and remove software packages using the package manager relevant to a chosen Linux distribution.

   Ans: A step-by-step guide to install, update, and remove software packages using **dnf** package manager for the Fedora Linux distribution is as follows:

   Install application:

   a. Firstly, we have to enter the Terminal.

   b. we have to update the dnf package manager using **sudo dnf update.** This will update the package manager to the latest version which has all the current versions of all applications.

   c. Then we have to type **sudo dnf install application-name**. After giving the password the program will be installed by the package manager. We might have to type yes or y to proceed with the rest of the installation after the package

manager asks for us to do it.

Update application:

a. First, we have to check if there is any update available for the specific application that we are trying to update using **sudo dnf check-update.** This command will list all packages with available updates. We have to look through the list to see if the application we want to update is mentioned.

b. If there is any newer version of the application we are trying to update we have to type **sudo dnf update application-name**. Note that we have to keep the application name the same as the name we have found in the list. It might include extra words or the current version number.

Uninstall application:

a. Firstly, we have to search for the specific application or package we want to uninstall using **sudo dnf search application-name** command.

b. Then we have to use the **sudo dnf remove application-name** command for uninstalling the application.

c. Note that, there could be several instances of the application that we are trying to install, so we can use the wildcard to uninstall all of them that have the same name. The command for it would be **sudo dnf remove application-name***

4. Provide examples of common log files, their locations, and the information they contain.

Ans: Log files on any Linux distribution, web servers, or mail servers are used for proper system administration, fixing any problems, and recording all the events of a system. We can understand if the system is running well or find out any threat to the system. Some of the most common log files, their locations, and the information they contain are as follows:

Fedora Log files: The log files of the Fedora Linux distribution are normally located in **/var/log** directory, which has key log files like messages, dnf log files, and system log files. These files contain security-related files, log file updates, and installation of packages.

Ubuntu System Log files: The log files of the Ubuntu/Debian-based Linux Distribution are located in **/var/log/syslog** directory. In these files, system messages such as startup messages, kernel messages, etc. are stored.

CentOS Authentication Log Files: The authentication log files are located at **/var/log/auth.log**. This includes user login authentication to the system, sudo access

requests while needed from admin, why the authentication failed, and when to determine any discrepancy or hacking attempt.

5. A system administrator needs to manage user accounts on a Linux server. Research the internet and explain the commands and procedures for creating, modifying, and deleting user accounts and groups.

   Ans: For creating a new user account, we have to first open the terminal, then we need to type **sudo useradd username.** This will give us the prompt to assign a password for the user.

   To modify the user accounts, we have to use the command **sudo usermod newusername oldusername.** In that a new username will be updated in place of the old username.

   To delete any user account, we need to run **sudo userdel username** command. This will add the current user whose name was given.

   For creating new groups where users can collaborate we can run **sudo groupadd groupname** command.

   For modifying the group name we can run the following command **sudo groupmod newgroupname oldgroupname.**

   For adding the user to a group we need to run the following command **sudo usermod -aG groupname username.** To delete a group we need to run **sudo groupdel groupname.**

Basic Programming Skills

1. Implement a python script that takes a user-provided password as input and evaluates it against the following conditions -
   - At least 8 characters in length.
   - Should contain a mix of uppercase and lowercase letters.
   - Must include at least one numeric digit
   - must include at least one special character from the set: **!@#$%^&*()-_=+[]{}|;:'",.<>/?.**

   Ans:

```
def password(pas):
    has_lower = False
    has_upper = False
    has_digit = False
    has_spec = False
```

```
    for char in pas:
        if char.islower():
            has_lower = True
        elif char.isupper():
            has_upper = True
        elif char.isdigit():
            has_digit = True
        elif char in "!@#$%^&*()-_=+[]{\}|;:'\",.<>/?":
            has_spec = True

    if (len(pas)) >= 8:
        if has_lower:
            if has_upper:
                if has_digit:
                    if has_spec:
                        return True

inp = input("Please, enter your password: ")

if password(inp):
    print("Password is valid!")
else:
    print("Invalid Password. Please try again!")
```

2. Write a Python script to encrypt and decrypt files using a cryptographic algorithm (e.g., AES). Users should be able to provide a key for encryption and use the same key for decryption.

   Ans: Could not Finish

Cybersecurity Basics

1. A company has noticed an increase in phishing attempts targeting its employees. Research and outline the common techniques used in social engineering attacks.

   Ans: Phishing is the type of network security threat that deceives people into giving personal information by pretending to be a trustworthy entity. In the case of a company, it could be a critical threat, since if one person from the company clicks on a phishing link it can get inside the company network. Types of social engineering attacks are as follows:

Spear phishing: It is a type of phishing attack that attacks specific individuals or companies. This type of attack is used to steal confidential information which is of importance to the attackers.

Voice phishing: This type of phishing uses phone calls to scam the user for private information. Attackers pretend to be a legitimate organization, or tax official where they try to claim that there is an issue with the victim's information that needs to be solved fast.

Pretexting: It is a type of social engineering in which victims are persuaded to reveal sensitive and important information by creating convincing cover stories.

Piggybacking: Tailgating is the practice of an unauthorized person using an authorized person's credential to get inside a system or restricted page of the application to gain confidential information.

2. Imagine a scenario where a company's computer systems have been infected with malware. Research and propose a detailed strategy for defending against malware attacks.

   Ans:

   Creating awareness among employees: Conducting regular training sessions on identifying phishing attempts, and the importance of not downloading any unauthorized software.

   Installing antivirus software: Ensuring that all devices are protected by antivirus software to detect and prevent malware infections.

   Security update devices regularly: Regularly updating operating systems, and applications on all devices to minimize security vulnerabilities.

   Advanced email filtering: Secure email gateways can be used to detect any phishing emails and use anti-phishing applications and browser extensions on the devices.

   Monitor network traffic: Using proper network monitoring tools to identify unusual activity that could indicate a malware infection.

   Threat isolation: If any malware is detected, they can apply proper containment measures based on the type of malware. This might involve disabling certain services, deleting malicious files, or applying specific security patches, and isolating the infected systems.

3. A small business is concerned about the security of its network. Research and suggest basic network security measures, including the use of firewalls, intrusion detection systems, and encryption. Provide a step-by-step guide on implementing these measures and explain how they contribute to a secure network environment.

   Ans: Basic network security measures would include strengthening the firewalls, adding a proxy network using VPN for safe and encrypted internet use, and using passive intrusion detection systems that can detect anomalies.

   Firewall: It acts as a barrier between your internal network and the internet. It controls the incoming and outgoing traffic based the certain security rules. Normally, a firewall comes with a Windows operating system but it is also present in other OS. Regularly updating the firewall will keep it to the latest version and new types of network threats will be blocked by an active firewall.

   Intrusion Detection System: Intrusion detection system or IDS for short is used for monitoring network traffic. It is a passive application that can used for checking for any suspicious process or potential threat in the network. For using an IDS firstly, we have to identify what type of IDS we want to use. There are NIDS that need to be placed at a strategic point within your network to monitor traffic across the devices. Comparatively, we have to install HIDS in the critical server or endpoints. Properly configuring the IDS will reduce the errors that can confusion.

   Encryption: Properly encrypting the data storage into a coded format can make it unreadable to unauthorized users. This can be achieved by different encryptions that are available online.

   Proxy Network: Using a secure proxy network, authorized employees can work without thinking about any network threats. All the data will be filtered by the proxy network.

   Secure Wi-Fi Networks: Secure wifi passwords using WPA3 or later encryption can keep the wifi network across the company protected. Properly hiding the network SSID and protecting the network with a strong password will keep hackers at bay.

   Strong Password Policy: Creating awareness among the employees about a strong and unique password policy will help ensure proper security.

   VPN: Using a Virtual Private Network or VPN to surf across the web or during data transfer is a secure option for any business.

Web Technologies

1. A development team is tasked with building a data-intensive web application. Conduct an in-depth technical comparison of three web development frameworks (e.g., Django,

Ruby on Rails, Express.js). Evaluate their ORM capabilities, routing mechanisms, and support for RESTful APIs. Recommend the framework that aligns best with the project's technical requirements and scalability needs.

Ans: Django**,** Ruby on Rails, and Express.js are the most commonly used web development frameworks at present. I have discussed them keeping in mind Obejct Relational Mapping (ORM) capabilities, routing mechanism, and support RESTful APIs.

Django: Django is a Python-based and open-source backend framework that is great for data-intensive applications. It comes with a pre-built ORM that allows developers to create data models from scratch. It uses a URL dispatcher for routing, which makes it efficient for mapping URLs to callback functions. Django has its own Django Rest Framework or DRF for short which is a powerful tool for building APIs.

Ruby on Rails: It is a server-side website application framework written in Ruby programming language under an MIT license. It is a feature-rich framework that forces the developer to reuse components under several rules. The ORM of Ruby on Rails is called ActiveRecord. ActiveRecord supports various databases and includes a comprehensive query interface. Ruby on Rails uses a RESTful routing approach, encouraging the development of RESTful APIs within its applications. That is why it is easy to build Restful APIs, due to its REST-orientated routing logic.

Express.js: Express.js is a backend framework for building RESTful APIs with Node.js. It does not come with a built-in ORM but it supports middleware like Mongoose for MongoDB connection and Sequlize for SQL-related database. However, it requires support from Django or Ruby to properly utilize the complex data operations. Express provides minimalistic routing capabilities. It allows for the definition of routes based on HTTP methods or URLs straightforwardly.

So by comparing the above three frameworks, I feel like Django would be an ideal choice between the three for data intensive work. Since the ORM of Django would give us the support to create data models from scratch. It is also ideal as it has clean routing mechanisms and a powerful Django Restful Framework for building RESTful APIs. That is why it would be the best choice to use for the data intensive web application.

2. What are Content Security Policy (CSP) & Cross-Origin Resource Sharing (CORS), and why do we require these?

Ans: Content Security Policy (CSP) is an additional layer of protection that helps in the detection and mitigation of certain attack types, such as data injection and cross-site scripting or XSS attacks. These kinds of attacks are used for various purposes, such as malware distribution and data theft. With the help of CSP, we can prevent ourselves from this kind of attack which can steal or corrupt our confidential information.

Cross-Origin Resource Sharing (CORS) is a mechanism guided by HTTP headers that enables a server to specify which origins (domain, scheme, or port) other than its browser is allowed to load resources from. CORS also utilizes a preflight request process where browsers inquire about the server hosting the cross-origin resource to verify if the actual request is allowed. This policy prevents malicious websites from accessing private data on another domain without permission. It ensures that sensitive information can only be shared with authorized domains, thus enabling more secure web application architectures without compromising security.

3. Mention the risks (2 for each platform) while using popular CMS options - Wordpress, Joomla, Drupal

   Ans: The risks of each platform are as follows:

   WordPress:

   a. **Outdated Plugin:** As we know there are a lot of plugins in WordPress to choose from. But it also possesses risks since outdated plugins could have security vulnerabilities. Hackers can make use of these sorts of vulnerabilities and steal sensitive information.

   b. **SQL Injection attacks:** Because WordPress runs on a database, it also uses PHP server-side scripts. This gives a chance to URL insertion or SQL injection attacks. When someone enters malicious SQL code into a website's database, it's known as a SQL injection attack. It is possible to obtain private data or even take over the website with the help of malicious code.

   Joomla:

   a. Late updates: Joomla only gives after vulnerabilities are discovered. So, it is possible to be attacked by hackers before the updates are installed.

   b. Bad Extension Security: Similar to WordPress, Joomla extensions can also be a weak link for security. Outdated extensions can cause vulnerabilities and can be exploited by hackers.

   Drupal:

   a. **SQL Injection:** Due to structural complexity Drupal is ideal for SQL injection attacks. Such attacks can allow attackers to interfere with the queries that an

application makes to its database, potentially accessing sensitive information.

b. **Access control issues:** In Drupal, problems with access control arise when users are given more permissions than they require. This may result in unauthorized access to private information or features. To avoid problems with access control, user roles and permissions must be set up correctly.

Database Management

1. Research and outline best practices for securing a database, covering topics such as authentication, authorization, encryption, and auditing.

   Ans:

   The best practice for securing a database is carefully securing the most important things that are needed to run a proper database.

   Firstly, Authentication in a database verifies a user's identity before granting access to the database. It typically involves a username and password, but stronger database systems also use multi-factor authentication (MFA), adding elements like one-time passwords or biometric data to enhance security.

   Secondly, Authorization occurs after authentication, determining what an authenticated user can do within the database. This process involves setting permissions and privileges based on roles or individual user accounts, ensuring users access only the data and actions necessary for their role.

   Thirdly, Encryption protects data confidentiality, with data-at-rest encryption securing stored data and data-in-transit encryption safeguarding data as it moves across networks, preventing unauthorized access to readable data.

   Finally, auditing involves tracking and logging database activities This practice helps in detecting unauthorized activities, ensuring compliance with regulatory standards. Together, these practices form a comprehensive approach to database security, protecting sensitive information from unauthorized access, data breaches etc.

2. A data-intensive application is being developed to handle large volumes of unstructured data. Which NoSQL database options would be more suitable among - MongoDB, Cassandra, Redis in this situation?

Ans: For a data-intensive application handling large volumes of unstructured data, MongoDB would be the most fitting option among MongoDB, Cassandra, and Redis. MongoDB is document-oriented which means it can manage unstructured data in a flexible, JSON-like format. It also offers scalability through sharding and ensures strong consistency. While Cassandra provides excellent write scalability and fault tolerance for applications, and Redis offers unmatched speed with its in-memory storage, MongoDB's schema flexibility and comprehensive support for unstructured data handling aligns with the needs of a data-intensive application where large volumes of unstructured data is being handled.

Cryptography

1. What is PKI? Describe how PKI can enhance the confidentiality and integrity of communication in the financial sector.

   Ans: A public key infrastructure is the collection of roles, guidelines, resources, and practices required to manage public-key encryption and create, distribute, utilize, store, and revoke digital certificates.

   PKI uses asymmetric cryptography, which evolves a pair of keys, a public key, and a private key. This ensures proper encryption of the data which is very much needed for any financial organization. Using PKI we can issue digital certificates which ensures that only those with valid credentials can access sensitive data and applications, helping to prevent unauthorized access. It is essential to stop fraud in the banking industry. Institutions can guarantee that transactions are resistant to tampering and that the sender's identity is confirmed by utilizing digital signatures and certificates. In this way, PKI can enhance the confidentiality and integrity of communication in the financial sector.

2. A security analyst needs to recommend an encryption method for securing communication between two systems. Research and compare symmetric and asymmetric encryption methods. Discuss the strengths and weaknesses of each approach, considering factors such as key management, speed, and suitability for different use cases.

   Ans: Symmetric encryption uses a single key for both encryption and decryption, offering the advantage of speed due to simpler algorithms, which makes it suitable for encrypting large volumes of data. However, its key management can be challenging, especially in scenarios requiring secure key exchange over unsecured channels.
   On the other hand, asymmetric encryption employs a pair of keys public and private where the public key encrypts data, and the corresponding private key decrypts it. This method simplifies key distribution since public keys can be shared openly, enhancing security in communications across unsecured networks. However, asymmetric

encryption is slower than symmetric encryption due to the complexity of its algorithms, making it less efficient for encrypting large datasets.

The choice between symmetric and asymmetric encryption depends on the specific requirements of the use cases. Symmetric encryption is often preferred for internal data encryption and scenarios where secure, and efficient encryption is required for large data volumes. Asymmetric encryption is favored for secure communications over the internet, such as SSL/TLS for websites, where key exchange security is important.

However, it can also be possible to use both types of encryption where we will use symmetric encryption for data transfer and asymmetric encryption for secure key exchange.

3. Research and explain how digital signatures can be used for authentication. Provide a step-by-step guide on how digital signatures work

   Ans: A digital signature is a PKI-based digital certificate that verifies the signer's identity and guarantees that digital messages and documents sent electronically haven't been changed or fabricated. Asymmetric encryption is used in digital signatures to authenticate the identity of the message sender and ensure the integrity of the message.

   A step-by-step guide on how digital signatures is given below:

   1. In the document platform or application, the sender chooses which file to digitally sign.
   2. The sender's computer determines the file content's unique hash value.
   3. To construct the digital signature, this hash value is encrypted using the sender's private key.
   4. The original file along with its digital signature is sent to the receiver.
   5. The digital signature on the file is detected by the receiver using the appropriate document application.
   6. Finally, using the sender's public key, the receiver’s computer decrypts the digital signature.

Familiarity with Security Tools and Software

1. What kind of tasks can be performed using tools like - Snort or Suricata? Describe a scenario where these can be used.

Ans: Globally, two of the most widely used intrusion detection and prevention systems (IDS/IPS) are Snort and Suricata. To identify malicious activity on networks, both systems use protocol analysis, rules, and signatures.

These are intrusion detection systems (NIDS) that are network-based. Through the use of NIDS, which can identify malicious traffic throughout a network, enterprises can keep an eye out for questionable activity in their local, virtual, and cloud network environments. Both Snort and Suricata employ anomaly-based and signature-based detection. With signature-based detection, packets are compared to a pre-established ruleset, giving organizations highly accurate threat identification. On the other hand, by using machine learning to simulate baseline traffic patterns, anomaly-based detection, on the other hand, notifies organizations of outlier traffic.

Given a scenario, where hackers are trying to attack a company's network NIDS based application Snort or Suricata will be of big help to check whether there are any attacks or threats or not.

2. List 3 vulnerability scanning tools and compare them based on - features, price, and popularity.

Ans: Three vulnerability scanning tools are Tenable, Invicti and StackHawk.

Features: Tenable is renowned for its comprehensive vulnerability scanning capabilities, offering high-speed discovery, configuration auditing, asset profiling, sensitive data discovery, and vulnerability analysis.

With the fewest false positives compared to other scanners, Invicti offers the widest range of website and application vulnerability scans, cutting down on lost time. Efficient processes can be achieved by integrating the robust scanner with common development pipeline tools and offering automated on-premises or SaaS-hosted scanning.

StackHawk focuses on smaller or less experienced DevOps teams with its more constrained scanning choices, To facilitate quick corrections and enable triage of discoveries, the highly focused DAST scanner connects with Slack and CI/CD automation.

Price:

Tenable offers different pricing tiers, starting with Nessus Essentials, which is free for up to 16 IP addresses. The more advanced version, Nessus Professional, is priced at approximately $2,990 per year.

Instead of disclosing prices, Invicti sells licences on the number of scanned websites and user seats. Among the three licencing tiers are:

- Standard: Offers one user's desktop scanner installation on-site.
- Team Licence: Offers continuous access for many users, as well as features for asset discovery, PCI compliance, and integrated workflow tools.
- Company: Access to hosted and on-premises deployments, customised workflows, and specialised tech support are all made possible by licences.

Stack Hawk offers four DAST licensing levels with monthly or annual billing. The Free Tier supports DAST for one app with CI/CD integration. The Pro Tier, at $49/month per developer (minimum five), provides unlimited scans, more integrations, and support via email or Slack. The Enterprise Tier, at $69/month per developer, adds features like single sign-on, API access, and premium support options including dedicated Slack and Zoom. Custom pricing is available for large teams, offering volume discounts.

Popularity: Among the three scanners Tenable is the best choice as it can perform vulnerability scans in Network, Endpoint, and Server websites and Application-based IoT.

3. What kind of tool is Autopsy? What can be done using this software?

Ans: Autopsy is a digital forensics software that is used to identify what happened on a digital device. This is mainly used by law enforcement agencies, military, and corporate examiners. We can use it for data recovery, timeline analysis, keyword searching, registry, and file system analysis using this tool. This sort of functionality of Autopsy can be used for criminal and corporate investigations.